Penn Medicine
Lancaster General Health

# POLICY TITLE: Access Controls for Information Assets
## Former Policy Title: Computer Access

## POLICY PURPOSE:

To establish access controls for Lancaster General Health (LG Health) information assets.

## POLICY STATEMENT:

Information assets will be managed using the minimum access control requirements identified in this policy as well as any associated policies, procedures, or standards. More stringent and/or additional access controls may be utilized where appropriate.

1. Information assets should only be available to authorized individuals or ‘users’.
2. Data classification standards will be considered when determining minimum access control requirements.
3. The administration of access control roles will be segregated where possible (e.g., access request, access authorization, and access administration).
4. Relevant accreditation and/or regulatory requirements as well as contractual obligations regarding protection of access to data or services will be taken into consideration; and
5. The requirements of individual business unit(s) or department(s) will be taken into consideration.

Exceptions to this policy will be approved by the appropriate Information Management Internal Controls Oversight Committee.

## APPLICABILITY/SCOPE/EXCLUSION:

This policy is applicable to all LG Health information assets.

## DEFINITIONS:

**Access Controls –** Procedures and technical controls that designate access to information assets. These controls may be accomplished through physical access limitations, software, authentication, or authorization procedures.

**Information Assets –** An application, system or solution that creates, receives, maintains, stores or transmits confidential information, such as Protected Health Information (PHI), personally identifiable information (PII), payment card data, usernames and passwords, company proprietary business plans or financial data, etc., the confidentiality, integrity and availability of which must be safeguarded for the sake of overall business risk management. Information assets may be physical or virtual and include, but are not limited to: the LG Health network, a physical device or hardware, storage media, software, data, reports or summaries.

## PROCEDURE:

LG Health will apply the following information access control principles:

A. **Least Privilege**: Access privileges for users are limited to only what is necessary to be able to complete their assigned duties or functions. Role based access (RBA) will be implemented unless an exception has been documented and approved.

B. **Minimum Necessary**: Access to confidential information is limited to that information required to perform a particular business activity or to achieve an authorized requestor's specified purpose. Minimum necessary is based on the need-to-know principle.

C. **Segregation of Duties**: Whenever practical, no one person is responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

Access controls will be supported by formal policies, procedures, standards and/or guidelines that address the following:

1. **Authorized Access to Information Systems**
   To ensure user accounts are created, managed, and periodically reviewed to prevent unauthorized access to information systems, the following standards will be referenced:

   - **Password Standards and Guidelines**
   - **Role Based Access Controls Management Guidelines**

2. **User Responsibility**
   The user's responsibility is defined in other policies, including the **Safeguarding Confidential Information** and **Acceptable Use of Electronic Resources** policies. All users must sign a confidentiality agreement in order to obtain access to information assets and the corporate network.

3. **Privileged Access Controls**
   Privileged Accounts (e.g., administrator accounts) will be managed according to the **Privileged Account Management** policy.

4. **Device Level Access Controls**
   - **Device Inventories** will maintained by Information Services.
   - **Physical safeguards** will be used to minimize unauthorized viewing of content and theft or loss of devices.
   - **Encryption** will be used on all mobile devices and removable media. See **Portable Computer Management** and **Safeguarding Confidential Information** policies.
   - **Secure Log-on** procedures will control access to operating systems.
   - **Use of System Utilities** or utility programs that might be capable of overriding system and application controls will be restricted and tightly controlled.
   - **Screensavers** will be enabled to prevent incidental viewing of confidential information.

- **Session Time-out** - Inactive sessions will terminated after a defined period of inactivity.

5. **Application Level Access Controls**
   - When possible, applications should provide a method for limiting a user's level of access to only what is required to perform a job function and support role based access according to the **Role Based Access Guidelines**.
   - Applications will be configured to automatically Lock (secured) or Log Off according to the **Application Idle Timeout Guidelines**.
   - Applications will be configured to:
     - **Expire user passwords** at a maximum of 180 days.
     - **Disable access** after a maximum of 90 days of inactivity.
     - **Lock Out** user access after three consecutive incorrect password attempts.

6. **Physical Access Controls**
   Physical access controls will be used, as appropriate, to limit or restrict access to prevent unauthorized physical access, tampering, and theft. Physical Access controls include controlled entry doors, alarms, and video surveillance,

7. **Remote Access Controls**
   Remote access will be controlled as described in the Remote Access Policy.

## ROLES/RESPONSIBILITIES:

**Information Services** is responsible for providing technical review and where approved/required, the technological solutions needed to support adherence to policy**.**

**Directors/Managers/Access Authorizing Agent(s)** are responsible for approving or denying of requests for the activation, modification, and deactivation of user access.

**Director, Information Assurance** is responsible for achieving compliance, managing exceptions, as well as coordinating implementation activities, training, and enforcement actions as needed.

**System Administrator(s)**, as defined within the IS Application Database and in cooperation with Identity and Access Staff, are responsible for the operational maintenance of user accounts including the activation, modification, monitoring, and deactivation of accounts for their respective applications. This includes monitoring and acting upon workforce member termination and job transfers in a timely fashion. In addition, System Administrators are responsible for following standards according to the **System Administrator Standards**.

## APPENDICES: N/A

## FORMS: N/A

## REFERENCES:

HIPAA Administrative Safeguards §164.308; HIPAA Technical Safeguards §164.312; The Joint Commission Information Management Standards

Acceptable Use of Electronic Resources Policy
Safeguarding Confidential Information Policy
Privileged Account Management (Information Services Department Policy)
Password Standards and Guidelines (Information Assurance Department Standard)
Role Based Access Controls Management Guidelines (Information Assurance Department Standard)
System Administrator Standards (Information Services Department Standard)